Seers and Craftspeople

Steve Bellovin
Columbia University

The security research business is in trouble. Yes, it's producing all sorts of fascinating new papers, ones that demand to be read. I count a conference a success if I get one neat new idea of my own to think about; at one recent conference, I got two in one day. The problem, though, is what effect these papers (or my own new ideas from them) are likely to have on real-world security problems. On that, I'm becoming pessimistic.

The question I'm asking now, and the reason for my pessimism, is rather different than, "Is this or is this not a really cool idea?" It's more pragmatic: "How likely is it that this paper will make our systems noticeably more secure?" I find it hard to answer that question in the affirmative for at least three reasons: past successes, intractable problems, and structural issues.

The bright side of the coin is that we've had a lot of success thus far. This is most evident in cryptography, in which theorists have supplied practitioners with far more tools than have been deployed. Modern ciphers, if properly used, appear to be unbreakable. Consider the Data Encryption Standard (DES): in more than 30 years, exactly one attack stronger than brute force has been found, and it's probably impractical. In fact, the only practical attack—brute force—was arguably an intentional weakness.

We've even seen noticeable success in dealing with bugs. It's no longer a shock to see a computer that has gone more than a year without a reboot. By contrast, the mainframes I used 40 years ago were prophylactically rebooted every morning and generally crashed once or twice in between. Because bugs are the primary cause of security holes, this is indeed quite significant. Unfortunately, we still have far to go in this direction.

Fundamentally, writing correct code is *hard*. As Fred Brooks pointed out in his seminal essay, "No Silver Bullet"—which you can find in his *The Mythical Man-Month* (Addison-Wesley, 1995)—it isn't realistic to expect an order-of-magnitude improvement in software productivity in the course of a decade. I'll make a stronger claim: buggy code is not only the oldest unsolved problem in computer science, it will remain so. We'll never have bug-free code—and bugs are, as noted, the leading cause of security problems.

The structural problems in the security field are in some sense both the easiest and the hardest to tackle. In Lee Smolin's provocative book *The Trouble with Physics*: *The Rise of String Theory, the Fall of a Science, and What Comes Next* (from which I stole the title of this essay), he drew a distinction between *seers*—those who step outside of the current paradigm and orthodoxy to teach us a different way to approach problems—and *craftspeople*—those who fill in the missing pieces in the grand theories that the seers create. (I'm not qualified to judge Smolin's assessment of physics; for now, let it suffice to say that he claims that the deity of your choice doesn't play Cat's Cradle with the universe.) Craftspeople are very necessary; without them, we can't use the seers' products. But craftspeople don't lead us out of the swamp when we're lost.

Some of this dichotomy is cyclic. Once we have a revolution in thought, it takes a while for the craftspeople to let us use the new tools and see their limits. Then, and only then, is there soil fertile enough to grow new seers. Much of the problem, though, lies in the way we judge research. Peers—grant reviewers, tenure committees, conference organizers—tend to judge according to the current orthodoxy. A brilliant but flawed paper—one that boldly moves in a new direction but obviously ignores some issues or even creates new ones—is likely to be rejected. After all, it has blatant flaws, and its new ideas are unproven.

This is the danger we have to avoid. We need to judge new ideas more by their potential to escape today's dead ends, and less by what they leave unsolved. If the ideas are good, a new generation of craftspeople can make them useful. □

Steve Bellovin *is a professor of computer science at Columbia University. He has a BA from Columbia University and an MS and PhD from the University of North Carolina at Chapel Hill. Bellovin helped create netnews, or usenet news, and is coauthor of* Firewalls and Internet Security *(Addison-Wesley, 2003). Contact him via www.cs.columbia.edu/~smb/.*